REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

In the specification, paragraphs 0007, 0009, and 0034 have been amended.

Claims 8 and 24 are currently being amended.

This amendment adds, changes and/or deletes claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending the claims as set forth above, claims 1-12. 15-40, and 42-68 are now pending in this application.

In the outstanding Official Action of September 8, 2006, the Examiner objected to the disclosure for various informalities. In particular, the Examiner identified paragraphs [0007], [0009], and [0034] as having minor grammatical and typographical errors. Applicant has amended paragraphs [0007], [0009], and [0034] of the specification in accordance with the Examiner's suggestion for clarification purposes. In addition, Applicant has identified and corrected another minor grammatical error at paragraph [0043]. If the Examiner has any further issues, he is invited to contact the undersigned.

The Examiner objected to claim 24 for containing a presumed typographical error. In response to the Examiner's objection, Applicant has amended claim 24 in accordance with the Examiner's suggestion. Namely, the limitation at issue now states, "at least one of a master secret code and at least one signature."

In the September 8, 2006 Official Action, the Examiner rejected claims 1, 3-12, 15-19, 21-24, 27-40, 42-44, and 46-68 under 35 U.S.C. §103(a) as being unpatentable over PCT Publication WO97/24831 (Ichikawa) in view of European Patent Publication EP 0538216 (Anvret et al.) and US Patent No. 6,240,512 (Fang et al.) Claims 2, 20, 25, 26, and 45 were

rejected under 35 U.S.C. §103(a) as being unpatentable over Ichikawa in view of Anvret et al, Fang et al., and US Patent No. 5,845,519 (Weiss). Applicant traverses the rejection for the reasons set forth below.

As has been discussed previously, the currently-pending claims describe a master secret key or code which is generated or calculated by a wireless communication device to calculate a signature, which is then transmitted to a data communication apparatus. The generation or calculation of the master secret key or code occurs in response to the wireless communication device receiving a message from the data communication apparatus, with this message including information such as the data communication apparatus's public key. The master secret key or code can then be determined by the data communication apparatus based upon information it already has in its possession. The calculated master secret key or code is then saved on the memory or memory means for later use. As has been discussed at length, this saving of the calculated code provides the benefit of the wireless communication device not having to regenerate or recalculate a master secret key or code at a later time, saving valuable computational resources.

Regarding Ichikawa, the Examiner asserted that Ichikawa teaches all of the required limitations of claim 1[1], except for the use of public and private keys. Applicant respectfully disagrees with the Examiner's position. In particular, Applicant submits that Ichikawa does not teach or even suggest operation with regard to a wireless communication apparatus communicating using a wireless application protocol nor any sort of operation including and in response to a chosen algorithm. Ichikawa merely teaches a system and method of generating data encryption keys in conjunction with a smartcard. (*See, e.g.,* Abstract). Although Ichikawa briefly mentions that smartcards are used in conjunction with wireless telecommunications technology, this admission is done only in the background of the specification. (*See,* page 2, lines 16-25). Nowhere else in the specification of Ichikawa is

[1] It should be noted that although claim is discussed, Applicant's arguments contained herein apply to other independent claims as applicable. However, Applicant disagrees with the Examiner's assertion at page 8 of the outstanding Official Action that claims 5, 15, 19. 22-24, and 46 "each recite limitations recited in, and are substantially equivalent to, Claim 1." (emphasis added). The remaining independent claims 5, 15, 19, 22-24, and 46 may have certain limitations in common independent claim 1, but also contain other limitations and/or features not recited in independent claim 1.

telecommunications discussed, let alone wireless telecommunication apparatuses and wireless application protocols. In fact, the entire specification, and all of the embodiments described by Ichikawa refer to a smartcard implemented as an Automatic Teller Machine (ATM) card which can be physically inserted into an ATM machine for retrieving cash. (*See, e.g.,* page 2, lines 3-15, page 10, lines 14-17, and page 13, lines 21-29). Therefore, Applicant submits that it is improper for the Examiner to assert that the substantive embodiments described in Ichikawa referring to ATM cards can blindly be applied to smartcards used in wireless telephony apparatuses. In contrast, claim 1 of the present application explicitly requires that a wireless communication apparatus is to be securely connected to a data communication apparatus based on a wireless application protocol.

In addition, claim 1 requires connecting a wireless communication apparatus to a separate unit, where the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, the request comprising information of which at least one pre-defined algorithm the wireless communication apparatus supports. As noted above, Ichikawa merely discloses operations regarding a smartcard, where the smartcard is implemented as an ATM card to be physically inserted into an ATM machine. There is no wireless communication apparatus or otherwise disclosed by Ichikawa, as all of the operations described are performed with, using, or from the perspective of the ATM card. Consequently, if the Examiner is reading the ATM smartcard of Ichikawa as the claimed "separate unit," the Examiner has failed to address the limitation of the wireless communication apparatus wherein the claimed separate unit is included.

Furthermore, Ichikawa never describes sending, within any request from a wireless communication apparatus, information regarding at least one pre-defined algorithm that the wireless communication apparatus supports. The Examiner cites page 10, line 14-page 11, line 11 of Ichikawa in support of his position. However, this portion of Ichikawa only describes a user physically placing an ATM card within a bank's ATM machine (the Examiner has not cited any technology teaching wireless ATM transactions), where a client, i.e., the smartcard requests access to a server, i.e., the bank's ATM machine. (*See,* page 10, lines 14-24). Afterwards, certain processes take place, where selected series number (SSN) 116 is selected using a selection algorithm for specifying a series number (SN) to be used in a

current ATM transaction. The SSN 116 is made known to the client/ATM smartcard, but Ichikawa never mentions sending information regarding the selection algorithm itself. (*See,* page 11, lines 1-8). In addition, although Ichikawa briefly alludes to an initialization transaction between the bank's ATM machine and the ATM smartcard, the initialization transaction, whatever that may refer to, occurs "before the processing of the flowchart of Figure 2," (emphasis added) where Figure 2 refers to the operation described above where the ATM smartcard first accesses the bank's ATM machine and performs the operations that the Examiner asserted read on those disclosed in claim 1. (*See,* page 11, lines 8-11). Therefore, an ATM smartcard taught by Ichikawa cannot indicate at least one algorithm with a request for access because Ichikawa explicitly teaches that the algorithm is already determined before the ATM smartcard/client ever requests access to the server/bank's ATM machine, not to mention that no wireless apparatus is taught by Ichikawa with which to support the at least one algorithm. In contrast, and contrary to the Examiner's assertion, claim 1 of the present application requires that the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, the request comprising information of which at least one pre-defined algorithm the wireless communication apparatus supports.

In addition, the Examiner asserted that Ichikawa teaches a data communication apparatus choosing an algorithm and transmitting a message which includes information about the chosen algorithm, citing page 9, lines 13-23 for support. Applicant submits that no such recitation is made in the cited portion of Ichikawa. Ichikawa merely describes passing a chosen SSN 116 to the ATM smartcard, not a chosen algorithm. Although Ichikawa refers to a "selection" algorithm, the term selection refers to the ability of the algorithm to select a SSN 116, not that it is a selected or chosen algorithm itself. Moreover, the operation described on page 9, lines 13-23 is merely an overview of the same operation which is described in greater detail on page 10, line 14-page 11, line 18. Therefore, although the Examiner interpreted the operation at page 9, lines 13-23 as an additional operation to the one described at page 10, lines 14-24, it is not the case. In contrast, claim 1 discloses one operation when the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, the request comprising information of which at least one pre-defined algorithm the wireless communication apparatus supports. In

addition, another operation is disclosed where upon reception of the request, the data communication apparatus chooses at least one algorithm associated with a public and private key, and transmits a message back to the wireless communication apparatus, the message comprising the public key and information about which algorithm the data communication apparatus has chosen.

The Examiner further asserted that Ichikawa contemplates a wireless apparatus that generates a master secret code and calculating a signature based on a chosen algorithm and the master secret code and cited page 4, lines 10-15 for support of his position. Applicant submits yet again, that no wireless apparatus is disclosed in Ichikawa, let alone one that generates a master code. In addition, page 4, line 12 of Ichikawa describe a scenario where a derived key (DK), which the Examiner interpreted as reading on the claimed master secret code, is used in a second algorithm. Page 4, lines 13-15 of Ichikawa further states that, "This second algorithm is used to encrypt data that is to be exchanged with an external system, or used to authenticate access. It may also be used to generate an electronic signature." It is unclear whether Ichikawa is suggesting that the DK is used to generate an electronic signature, or if it is the second algorithm that is used to generate the electronic signature. It should be noted that this reference to electronic signatures is only made in the Summary portion of the specification, and nowhere else in the specification. Therefore, even though Ichikawa mentions electronic signatures, no substantive description is made regarding them, i.e., operation or functionality therewith, specifics of its derivation from the DK if it is in fact derived from the DK, etc. Hence, it is improper for the Examiner to impart significant weight to such a disclosure due to the very brief and very generalized allusion thereto. Moreover, even if Ichikawa teaches that the DK is used to generate the electronic signature, no mention of an algorithm is made. In contrast, claim 1 requires that the wireless communication apparatus generates a master secret code and calculates a signature based in part, on the chosen algorithm.

The Examiner correctly recognized that Ichikawa does not teach the use of public and private keys. However, the Examiner asserted that Anvret et al. teaches the use of such keys and that it would have been obvious for one of ordinary skill in the art to have used the public and private keys of Anvret et al. in the invention of Ichikawa. Applicant respectfully submits

that although Anvret et al. discusses the use of public keys, private keys as described in the context of claim 1 are not taught. Anvret et al. teaches a system and method of identification and exchange of encryption keys for use in a standard identification and exchange procedure. (*See, e.g.,* Abstract and Column 5, lines 8-21). Although Anvret et al. suggests utilizing public RSA keys which are stored on a user's smart card, the use of private keys is not taught. At page 3 of the outstanding Official Action, the Examiner asserted that Anvret et al. was used, not for teaching a master secret code, but for teaching public and private keys. Although the Examiner noted the storage of two variables, "a" and "q," Applicant is unsure as to the applicability of such variables to the Examiner's assertions as they are merely two system constants used in calculating a key. (*See, e.g.,* Column 5, lines 53-57). In addition, Applicant assumes that the Examiner in asserting that Anvret et al. teaches the use of a "private key" is referring to a variable D, because Column 6, lines 47-48 teach encrypting a random number, R using a secret key, D, which results in an encrypted, random number, X. However, like Ichikawa, D is used to encrypt a random number, and is not associated in any way with a chosen algorithm. Furthermore, again, like Ichikawa, Anvret et al. teaches exchanging identities, public keys, and signatures upon initial contact between two users. In contrast, claim 1 of the present invention requires that the data communication apparatus chooses at least one algorithm associated with a public key and a private key, and that only upon reception of the response comprising the signature, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received and the private key, where the signature is calculated in response to a message sent by the data communication apparatus after choosing an algorithm from information comprising at least one algorithm sent in a request by the wireless communication apparatus. Therefore, Anvret et al. does not cure the already-discussed deficiencies of Ichikawa.

The Examiner also correctly recognized that neither Ichikawa nor Anvret et al. teaches generating a master secret code specifically in response to a message. However, the Examiner asserted that Fang et al. discloses such a method, citing Column 9, lines 9-15 of Fang et al. for support of his position. Applicant disagrees with the Examiner's assertion. Fang et al. teaches a system method of consolidating multiple passwords and granting access to protected areas using single sign on (SSO) service that uses a master key generated by one

SSO server and pulled by other SSO servers as needed. (*See, e.g.,* Abstract, Column 2, lines 24-40, and Column 6, lines 43-56). Therefore, a user of the invention of Fang et al. is simply relieved of a duty to personally remember a plethora of access passwords. However, the SSO service is totally unrelated to establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol. In contrast, claim 1 is entirely about establishing such a connection. Although similar terminology is used in the cited prior art references, the operation, functionality, features, and technology context associated with the limitations and terms recited in, for example, claim 1 of the present application are wholly different from that described in the Ichikawa, Anvret et al., and Fang et al. references. Therefore, it is improper for the Examiner to assert that the features and/or terms taught in the cited prior art references read on the limitations of claim 1 without considering the features and/or terms in their entire and proper context. Establishing a secure wireless connection as described in claim 1, for example, entails complicated handshaking and authorization between wireless and data communication apparatuses. Hence, inclusion of the wireless application protocol language. For example, paragraphs [0029]-[0030] and [0044]-[0068] of the present application describe in detail this handshaking procedure involving the wireless application protocol. This is completely different from the ATM smartcard interaction with an ATM machine taught by Ichikawa, the landline-based DTMF and modem-related communications between landline telephony apparatuses taught in Anvret et al., and the SSO service taught by Fang et al.

In addition, even though smart cards and secure access, in a very generic sense, are discussed in Fang et al., Column 9, lines 9-15 describe nothing related whatsoever to an actual "message." All that is described in Fang et al. is that an administrator initiates generation of a master key, where a master key merely refers to an entity used to encrypt a plurality of user passwords, i.e., "Furthermore, the master key preferably is allowed to change, as initiated by sso administrators who have concerns about possible key exposure." (*See,* Column 9, lines 8-11). In fact, at page 3 of the outstanding Official Action, the Examiner explicitly stated that, "Third, the Examiner notes that nowhere is it suggested by the Examiner or Anvret that the variable 'X' referred to by Application would be considered to be a master secret code; in fact, the portion referred to by Applicant (column 7, lines 12-13

stating that X is changed for each session would itself imply that X is not, in fact a master key or code." (emphasis added). Therefore, by the Examiner's own admission, any key or other variable that can be changed at will is not a master key or code, or at least not one in the sense of a master key or code as claimed in the context of claim 1 of the present application. Therefore, Fang et al., contrary to the Examiner's assertions fails to teach generation of a master code in response to a message.

Furthermore, even if the master key of Fang et al. could be likened to the claimed master secret code, although Applicant makes no such insinuation, Column 9, lines 11-15 of Fang et al. teaches that master keys are generated and distributed among SSO servers. In contrast, claim 1 requires that a wireless communication apparatus generates a master secret code, where a calculated signature is sent to the data communication apparatus, and upon receipt of a response containing the signature, the data communication apparatus calculates the master secret code. Therefore, the master secret code in claim 1 is not merely generated at one server and passed along, but actually calculated, not to mention that a SSO server is not analogous to either a wireless communication apparatus or a data communication apparatus. Moreover, page 12, lines 25-27 of Ichikawa describes that a DK, which the Examiner asserted is analogous to the claimed master secret code, is generated by a client process, i.e., generated in the server and client. Following the Examiner's line of reasoning, the DK would then also have to be analogous to the master key of Fang et al., which as described above, is only generated at SSO servers, and distributed among the SSO servers. Therefore, combining the teachings of Fang et al. and Ichikawa would result in an inoperable combination because while the master key of Ichikawa is generated at both the client and server, the master key of Fang et al. is only generated at a server. That is, there is no resolution to the inherent operational conflicts that would exist between Fang et al. and Ichikawa.

In summary, neither Ichikawa, Anvret et al., nor Fang et al. teach at least: establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, where the wireless communication apparatus transmits a request to the data communication apparatus including information of which at least one pre-defined algorithm the wireless communication apparatus supports; the data communication apparatus choosing an algorithm associated with a public and private

key; calculating a signature based at least on the chosen algorithm; calculating the master secret code based on at least the chosen algorithm or in response to a message from the data communication apparatus; and/or generating a signature based on a master secret code and public key. Therefore, neither Ichikawa, Anvret et al., nor Fang et al. teach all of the required limitations of independent claims 1, 5, 15, 19, 22-24, and 46.

With regard to Weiss, Applicant submits that, because claims 2, 20, 25, 26, and 45 are all dependent upon the independent claims discussed above, each of these claims is allowable for at least the same reasons. However, Applicant wishes to separately note that Ichikawa unequivocally teaches that the master key used therein should be stored "in a secured area of permanent memory." (*See, e.g.,* page 4, lines 5-8). In other words, Ichikawa explicitly teaches storing a master key in a location such that is permanently stored. Therefore, Applicant submits that one skilled in the art would not be motivated to modify the invention of Ichikawa to have the master key stored for only a predefined period of time, because the Ichikawa reference itself instructs a person to have the master key permanently stored. Applicant therefore submits that these claims are patentable over the prior art for this reason as well.

For the above reasons, Applicant respectfully submits that none of the reference cited by the Examiner, either separately or in combination with each other, teach or suggest each element of independent claims 1, 5, 15, 19, 22-24, and 46. Therefore, Applicant submits that each of independent claims 1, 5, 15, 19, 22-24, and 46 are patentable over this prior art. Furthermore, because dependent claims 2-4, 6-12, 16-18, 20, 21, 25-40, 42-45, and 47-68 are all directly or indirectly dependent upon these independent claims, Applicant submits that these claims are patentable over the cited prior art as well.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 50-0872. Should no proper payment be enclosed herewith, as by a check or credit card payment form being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 50-0872. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 50-0872.

Respectfully submitted,

Date: March 7, 2007

By /G. Peter Albert Jr./

FOLEY & LARDNER LLP
Customer Number: 30542
Telephone: (858) 847-6735
Facsimile: (858) 792-6773

G. Peter Albert Jr.
Attorney for Applicant
Registration No. 37,268